Establishment of cryptographic keys in radio networks

Publication number: CN1179249

Publication date: 1998-04-15

Inventor: HASSAN A A (US); HERSHEY J E (US); CHENAKESHU S (US)

Applicant: ERICSSON GE MOBILE INC (US)

Classification:

- international: ***H04L9/16; H04B17/00; H04J13/00; H04K1/00; H04L9/08; H04Q7/38;*** **H04L9/14; H04B17/00; H04J13/00; H04K1/00; H04L9/08; H04Q7/38;** (IPC1-7): H04L9/08; H04B17/00; H04K1/00

- European: H04B17/00; H04J13/00; H04K1/00; H04L9/08

Application number: CN19961092682 19960119

Priority number(s): US19950376144 19950120

Also published as:

WO9622643 (A1)
EP0804839 (A1)
US5995533 (A1)
US5604806 (A1)
MX9705431 (A)

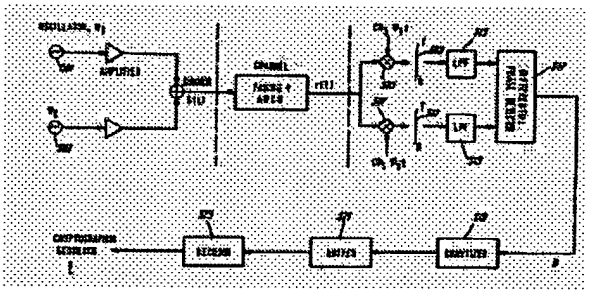
more >>

Report a data error here

Abstract not available for CN1179249

Abstract of corresponding document: **WO9622643**

Characteristics of the radio channel are used to establish key sequences for use in encrypting communicated information. These characteristics are the short-term reciprocity and rapid spatial decorrelation of phase of the radio channel. The keys can be established with computations equivalent to a bounded distance decoding procedure, and the decoder used to establish a key may be used for processing the subsequent data transmission. Compared to classical and public-key systems, an alternative mechanism for establishing and sharing key sequences that depends on a physical process is provided in which each party need not generate a pseudorandom quantity because the necessary randomness is provided by the temporal and spatial non-stationarity of the communication channel itself. By using a channel decoder, the probability of two users establishing the same secret key is substantially unity, and the probability of an eavesdropper establishing the same key is substantially zero. Also, the number of possible keys is large enough that finding the correct one by exhaustive search is impractical.



Data supplied from the ***esp@cenet*** database - Worldwide

[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 9/08
H04K 1/00 H04B 17/00

[12]发明专利申请公开说明书

[21]申请号 96192682.1

[43]公开日 1998年4月15日

[11]公开号 CN 1179249A

[22]申请日 96.1.19

[30]优先权

[32]95.1.20 [33]US[31]08/376,144

[86]国际申请 PCT/US96/00785 96.1.19

[87]国际公布 WO96/22643 英 96.7.25

[85]进入国家阶段日期 97.9.19

[71]申请人 艾利森公司

地址 美国北卡罗莱纳州

[72]发明人 A·A·哈森 J·E·赫尔希
S·陈那克舒

[74]专利代理机构 中国专利代理(香港)有限公司

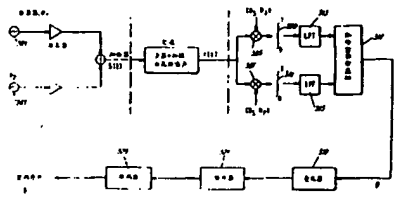
代理人 程天正 张志醒

权利要求书 5 页 说明书 21 页 附图页数 7 页

[54]发明名称 无线电网络中密钥的建立

[57]摘要

无线电信道的特性被用来建立在加密传送信息中使用的密钥序列。这些特性是无线电信道的相位的短期互易性和迅速的空间解相关。可以利用等价于有界距离译码过程的计算来建立密钥，可用建立密钥所用的译码器来处理随后的数据传输。与传统的系统和公共密钥系统相比，提供了建立和共享依赖于物理过程的密钥的替代机制，在这种替代机制中，因为通信信道本身的时间和空间非平稳性提供了必需的随机性，所以每一方都不需要产生伪随机数。通过利用信道译码器，两个用户建立相同密钥的概率基本上是1，而窃听者建立该同一密钥的概率基本上是零。还有，可能的密钥数目足够大，以致利用穷举搜索找出正确密钥是不实际的。



权　利　要　求　书

1.一种建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的方法，包括以下步骤：

在第一无线电收发信机中，发送多个正弦波信号，每一正弦波信号具有各自预定的频率和预定的初始相位；

在第二无线电收发信机中，检测第一无线电收发信机所发送的这些正弦波信号，并在预定时间周期之后发送这些正弦波信号；

在第一和第二无线电收发信机的每一个中，确定从另一无线电收发信机所接收的多个正弦波信号的每一个的相位；

在第一和第二无线电收发信机的每一个中，确定所接收的各对正弦波信号的相位之间的差值；

在第一和第二无线电收发信机的每一个中，把每一差值量化成为多个相位判决值中相应的一个；以及

在第一和第二无线电收发信机的每一个中，按照预定的分组码把多个量化差值译码成为一个密钥序列。

2.权利要求 1 的方法，其特征在于，还包括在第一和第二无线电收发信机的每一个中确定多个正弦波信号的每一个的振幅的步骤，这些振幅在译码步骤中被用作软信息

3.权利要求 1 的方法，其特征在于，还包括在第一和第二无线电收发信机的至少一个中根据密钥序列加密待发送信息的步骤；以及在第一和第二无线电收发信机的至少另一个中根据密钥序列解密所加密的发送信息的步骤。

4.权利要求 3 的方法，其特征在于，其中的加密步骤包括在信息流加密系统中组合密钥序列和要发送的信息的步骤。

5.权利要求 3 的方法，其特征在于，其中的加密步骤包括在面向分组的密码系统中组合密钥序列和待发送的信息的步骤。

6.一种建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的方法，包括以下步骤：

在第一无线电收发信机中，发送包括多个比特的预定数字字；

在第二无线电收发信机中，检测第一无线电收发信机所发送的该预定数字字，并在预定时间周期后发送该预定数字字；

在第一和第二无线电收发信机的每一个中，对从对方无线电收发信机所接收的预定数字字的多个比特中的每一个比特进行硬判决译码；以及

在第一和第二无线电收发信机的每一个中，按照预定的分组码把硬判决译码的这些比特变换成为密钥序列。

7.权利要求 6 的方法，其特征在于，还包括在第一和第二无线电收发信机的每一个中确定多个比特中的每一个比特的振幅的步骤，这些振幅在变换步骤中被用作软信息。

8.权利要求 6 的方法，其特征在于，还包括在第一和第二无线电收发信机的至少一个中根据密钥序列加密待发送信息的步骤；以及在第一和第二无线电收发信机的至少另一个中根据密钥序列解密所加密发送信息的步骤。

9.权利要求 8 的方法，其特征在于，其中的加密步骤包括在信息流加密系统中组合密钥序列和要发送的信息的步骤。

10.权利要求 8 的方法，其特征在于，其中的加密步骤包括在面向分组的密码系统中组合密钥序列和待被发送的信息的步骤。

11.一种建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的方法，包括以下步骤：

在第一无线电收发信机中，发送包括多个比特的预定数字字；

在第二无线电收发信机中，检测第一无线电收发信机所发送的该预定数字字，并在预定时间周期后发送该预定数字字；

在第一和第二无线电收发信机的每一个中，确定从另一无线电收发信机所接收的多个比特中的每个比特的相位；

在第一和第二无线电收发信机的每一个中，确定所确定的每一相位和相应的预定相位之间的差值；

在第一和第二无线电收发信机的每一个中，把每一差值量化成为多个相位判决值中相应的一个；以及

在第一和第二无线电收发信机的每一个中，按照预定的分组码把多个量化差值译码成为密钥序列

12.权利要求 11 的方法，还包括在第一和第二无线电收发信机的每一个中确定多个比特中的每个比特的振幅的步骤，这些振幅在译码步骤中被用作软信息。

13.权利要求 11 的方法，其特征在于，还包括在第一和第二无线电收发信机的至少一个中根据密钥序列加密待发送信息的步骤；以及在第一和第二无线电收发信机的至少另一个中根据密钥序列解密所加密发送信息的步骤。

14.权利要求 13 的方法，其特征在于，其中的加密步骤包括在信息流加密系统中组合密钥序列和待发送信息的步骤。

15.权利要求 13 的方法，其特征在于，其中的加密步骤包括在面向分组的密码系统中组合密钥序列和待发送的信息的步骤。

16.一种建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的设备，包括：

在第一无线电收发信机中，用于发送多个正弦波信号的装置，每一正弦波信号具有各自的预定的频率和预定的初始相位；

在第二无线电收发信机中，用于检测第一无线电收发信机所发送的这些正弦波信号、并在检测到开始之后的预定时间发送这些正弦波信号的装置；

在第一和第二无线电收发信机的每一个中，用于确定从另一无线电收发信机所接收的多个正弦波信号的每一个的相位的装置；

在第一和第二无线电收发信机的每一个中，用于确定所接收的正弦波信号对的相位之间的差值的装置；

在第一和第二无线电收发信机的每一个中，用于把每一差值量化成为多个相位判决值中相应的一个的装置；以及

在第一和第二无线电收发信机的每一个中，用于按照预定的分组码把多个量化差值译码成为一个密钥序列的装置。

17.权利要求 16 的设备，其特征在于，还包括在第一和第二无线电收发信机的每一个中用于确定多个正弦波信号的每一个的振幅的装置，这些振幅在译码装置中被用作软信息。

18.权利要求 16 的设备，其特征在于，还包括在第一和第二无线电收发信机的至少一个中用于根据密钥序列加密待发送信息的装置；以及在第一和第二无线电收发信机的至少另一个中用于根据密钥序列解密所加密发送信息的装置。

19.权利要求 18 的设备，其特征在于，其中的加密装置在信息流加密系统中组合密钥序列和待发送信息。

20.权利要求 18 的设备，其特征在于，其中的加密装置在面向分组的密码系统中组合密钥序列和待发送的信息。

21.一种用于建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的设备，包括：

在第一无线电收发信机中，用于发送包括多个比特的预定数字字的装置；

在第二无线电收发信机中，用于检测第一无线电收发信机所发送的该预定数字字并在预定时间周期后发送该预定数字字的装置；

在第一和第二无线电收发信机的每一个中，用于对从另一无线电收发信机所接收的预定数字字的多个比特中的每一个比特进行硬判决译码的装置；以及

在第一和第二无线电收发信机的每一个中，用于按照预定的分组码把硬判决译码的多个比特变换成为密钥序列的装置。

22.权利要求 21 的设备，其特征在于，还包括在第一和第二无线电收发信机的每一个中用于确定多个比特中的每个比特的振幅的装置，这些振幅在变换装置中被用作软信息。

23.权利要求 21 的设备，其特征在于，还包括在第一和第二无线电收发信机的至少一个中用于根据密钥序列加密待发送信息的装置；以及在第一和第二无线电收发信机的至少另一个中用于根据密钥序列解密所加密发送信息的装置。

24.权利要求 23 的设备，其特征在于，其中的加密装置在信息流加密系统中组合密钥序列和待发送的信息。

25.权利要求 23 的设备，其特征在于，其中的加密装置在面向分组的密码系统中组合密钥序列和待发送的信息。

26.一种用于建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的设备，包括：

在第一无线电收发信机中，用于发送包括多个比特的预定数字字的装置；

在第二无线电收发信机中，用于检测第一无线电收发信机所发送的该预定数字字并在预定时间周期后发送该预定数字字的装置；

在第一和第二无线电收发信机的每一个中，用于确定从另一无线电收发信机所接收的多个比特中的每个比特的相位的装置；

在第一和第二无线电收发信机的每一个中，用于确定每一所确定的相位和相应的预定相位之间的差值的装置；

在第一和第二无线电收发信机的每一个中，用于把每一差值量化成为多个相位判决值中相应的一个的装置；以及

在第一和第二无线电收发信机的每一个中，用于按照预定的分组码把多个量化差值译码成为一个密钥序列的装置。

27.权利要求 26 的设备，其特征在于，还包括在第一和第二无线电收发信机的每一个中确定多个比特中的每个比特的振幅的装置，这些振幅在译码装置中被用作软信息。

28.权利要求 26 的设备，其特征在于，还包括在第一和第二无线电收发信机的至少一个中用于根据密钥序列加密待发送信息的装置；以及在第一和第二无线电收发信机的至少另一个中用于根据密钥序列解密所加密的发送信息的装置。

29.权利要求 28 的设备，其特征在于，其中的加密装置在信息流加密系统中组合密钥序列和待发送的信息。

30.权利要求 28 的设备，其特征在于，其中的加密装置在面向分组的密码系统中组合密钥序列和待发送的信息。

说　明　书

无线电网络中密钥的建立

背景

本申请人的发明涉及安全地、也就是说不那么易于被窃听地传送信息的设备和方法。

在无线电通信系统中对于安全通信的广泛需求是显然的。仅举两个例子，与金融交易有关的信息利用无线电定期地进行交换，执法官员往往必需利用无线电传送语音和/或数据。在这两个例子中，尽管会有潜在的窃听者接收到强的信息信号，但几乎绝密地进行通信是关键的。蜂窝无线电话的用户也要求对他们的通信保密，而它们的通信可以在移动电话和基站之间的链路上或在移动电话之间的直接链路上进行。

提供安全性的一种方法是根据在使用之前用户已同意的某种方式加密所传送的信息。几种加密方法在文献中已得到描述，例如数据加密标准（ DES ）和公共密钥密码学（ PKC ），如 W. Diffie 等人发表在 Proc. IEEE（电气与电子工程师协会会刊）67 卷 397 - 427 页（ 1979 年 3 月）上的论文“保密与鉴权：密码学”中所描述的，传统的加密系统一般来说是能够按照各种各样的方式把明文（未加密信息）变换为密文或把密文变换为明文的一组指令、一个硬件或一个计算机程序，利用用户知道但对其他人保密的特定密钥选择其中的某一种方式。 DES 是传统的密码系统。

流行的 PKS 方式利用了这一事实：即容易通过计算找出一些大的素数，但难于通过计算对两个大素数的积进行因式分解。 PKC 系统优于其它密码系统（例如 DES ）之处在于 PKC 系统使用的解密密钥（两个大素数）与加密密钥（这两个大素数的积和一个相伴随数）。因此， PKC 用户的加密密钥可以公开供其他人使用，并避免了安全地分配密钥的困难。参见例如 R. I. Rivest 等人的“获取数字签名和公共密钥加密系统的方法”（ Commun.of the ACM（计算机协会通信），21 卷， 120 - 126 页， 1978 年 2 月），和 W. Diffie 的“公共密钥密码学的第一个十年”（ Proc.IEEE（电气与电子工程师协会会刊），76 卷， 560 - 577 页， 1988 年 5 月）。

对于传统的系统或 PKC 系统，消息的安全性在很大程度上取决于密钥的长度，如在 C. E. Shannon 的“保密系统的通信理论”所述的那样。（BSTJ（贝尔系统技术杂志），28 卷，656 ~ 715 页，1949 年 10 月）。

不幸的是，经常出现两个用户（例如两个警官）没有事先共享密钥、由此不能够利用传统的密码系统进行安全实时的通信的情况。即使 PKC 系统也需要用户产生伪随机数。此外，流行的 PKC 系统的安全性未经证实，并有在计算复杂性和必需交换大量信息方面蒙受严格要求的缺点。由于建立了破坏 PKC 系统的新方法，PKC 系统要重新处理比以往更长的交换矢量（实际上更大的素数）和比以往更复杂的计算。因此，传统的密码系统和 PKC 密码系统对于许多通信场合是不尽理想的。

由大气紊动干扰、用户的相对运动、来自建筑物和车辆等的变化的无线电信号反射所造成的无线电信道的易变性使任何无线电通信系统的任务复杂化。这种易变性造成传送信息的差错，并需要作出多方面努力来克服这些差错。例如，某些蜂窝无线电话系统把所要发送的模拟信息变换为数字信息，然后根据信息分组纠错码对数字信息进行变换。这种蜂窝无线电系统有北美数字先进移动电话业务（D - AMPS）和欧洲 GSM 系统，前者的一些特性由电子工业协会和电信工业协会（EIA/TIA）出版的 IS - 54B 和 IS - 136 标准进行规定。

在这种时分多址（TDMA）系统中，每一无线电信道、即无线电载波频率被分成一系列时隙，每一时隙包含来自数据源的信息的脉冲串，例如语音交谈的数字编码部分。分配给同一用户的顺序时隙（通常不是无线电载波上连续的时隙）构成用户的数字通信信道，该数信道可被看作是分配给该用户的逻辑信道。在每一时隙期间，可以发送 324 个比特，其中的 260 个比特的主要部分是编码器/译码器（codec）的语音输出，包括语音输出中的纠错编码用的比特。为了例如同步起见，其余的比特供保护时间和开销信令使用。

当前的其它蜂窝移动电话系统采用模拟 FM 方式来发送语音。三种主要的标准是美国的 AMPS 系统，使用信道之间的间隔为 30KHz 的宽带 FM，英国的 TACS 系统，信道间隔为 25KHz，以及斯堪的纳维亚的 NMT 系统，采用信道间隔为 12.5KHz 的窄带 FM。在努力减轻当前模拟 FM 系统的容量限制的过程中，D - AMPS 和 GSM 系统以及日本的系统都采用上述的数字传输，通过降低带宽要求来增大系统容量的另一

种方法是使用符合NAMPS规范的窄带FM系统，这种NAMPS规范规定了通过把 AMPS 的每一 30KHz 信道分割成为三个部分而实现的10KHz信道间隔。

图 1A、 1B 表示一示范性的多层蜂窝系统。用六边形（见图 1A）表示的伞状宏小区（ macrocell ）10是包括许多宏小区A1 ~ A7、B1 ~ B7（见图 1B）的覆盖蜂窝结构的一部分。每一伞状小区可以包含覆盖着的的微小区（ microcell ）结构。伞状小区和覆盖着的微小区的无线电覆盖可以重叠，或可以基本上不重叠。伞状小区 10 包括用在点线内包围的区域所表示的微小区 20 和用短划线包围的区域所表示的微小区 30，这相应于沿城市街道的区域，以及还包括覆盖建筑物的各层的微微小区（ picocell ） 40、 50 和 60。

简而言之，用控制信道来建立呼叫、通知基站有关移动台的位置和参数、以及通知移动台有关基站的位置和参数。基站监听移动台的呼叫接入请求，而移动台反过来监听寻呼消息。一旦接收到呼叫接入消息，就必需确定哪一个小区应对该呼叫负责。一般来说，这是根据在附近小区所接收的移动台的信号强度来确定的，然后由例如移动交换中心（ MSC ）命令指定的小区调谐到从一组可供该指定小区接入的话音信道中指定的一可用话音信道。

图 2A - 2C 表示按照 IS - 136 标准的在数字控制信道（ DCC ）上的示范性时隙格式。从移动台发送至基站的信息的两种可能的格式如图 2A 和 2B 所示，而从基站发送至移动台的信息的格式如图 2C 所示。这些格式基本上与在 IS - 54B 标准下供数字业务信道（ DTC ）所用的格式相同，但根据 1994 年 10 月 31 日提交的美国专利申请第 08/331,703 号给予每一时隙中的字段新的功能性，该美国专利申请在此被特意作为参考文献。在图 2A - 2C 中，在每一字段的上面表示了该字段中比特的数目。在 G、 R、 PREAM、 SYNC、 SYNC + 和 AG 字段中发送的比特按照通常的方式被用来帮助准确地接收 CSFP 和 DATA 字段，例如供同步、保护时间等使用。例如， SYNC 字段将与符合 IS - 54B 的 DTC 的 SYNC 字段相同，并载送由基站用来确定时隙的开始的预定比特格式。同样， SYNC + 字段要包括固定的比特格式，以便为基站提供附加同步信息，这种附加同步信息将在 PREAM 字段期间设定这些基站的接收机增益，以避免信号失真。

图 3 是供图 1A、 1B 所示的蜂窝结构和图 2A - 2C 所示的时隙使用的示范性蜂窝无线电话通信系统的方框图。该通信系统包括与相应的宏小区、微小区和微微小区之一相关的基站 110 、移动台 120 和 MSC140 。每一基站具有与 MSC140 进行通信的控制及处理单元 130 , MSC140 再与公用交换电话网（未示出）连接。每一基站还包括都被控制及处理单元 130 控制的至少一个话音信道收发信机 150 和控制信道收发信机 160 。移动台 120 包括与收发信机 150 、 160 交换信息的类似的话音和控制信道收发信机 170 和控制该话音和控制信道收发信机 170 的类似的控制及处理单元 180 。该移动台的收发信机 170 还与另一移动台的收发信机 170 交换信息。

进行通信的其它方法使用称为码分复用（ CDM ）和码分多址（ CDMA ）的系统。在普通的 CDMA 系统中，通过把要传送的数字信息序列与扩展序列组合而把该信息序列扩展或变换成为更长的数字序列。这样一来，该信息序列的一个或多个比特就用一系列 N 个“码片（ chip ）”值来表示。在这一过程（称为“直接扩展”）的一种方式中，每一扩展符号实质上是信息符号和扩展序列的乘积。在称为“间接扩展”的第二种形式的扩展中，各不同的可能信息符号由不同的不必相关的扩展序列代替。应当懂得信息符号可以由信道编码和/或扩展的一些前级来产生。

这种扩展的优点在于，只要用来表示不同信息源的信息序列的扩展序列彼此的干扰不太大，则来自许多信息源的信息可以同时在同一频带中进行发送。实际上，这些不同的扩展序列相当于不同的通信“信道”。一般来说，对于长度为 N 个码片，有 2^N 个可能的二进制扩展序列，这将形成非常大量的可能的 CDMA 信道。因为信道数不是如在相同带宽和数据速率的频分多址（ FDMA ）或时分多址（ TDMA ）系统中那样受 N 的限制，所以 CDMA 系统的这一特性有时被称为“软容量”。传统 CDMA 通信的各个方面的介绍请见 K. Gilhousen 等人发表在《 IEEE Trans. Veh. Technol 》（电气与电子工程师协会交通技术会刊） 40 卷 303 ~ 312 页（ 1991 年 5 月）上的论文“关于蜂窝 CDMA 系统的容量”，以及下面引用作为参考的美国专利文献：授权给 Dent 的美国专利 5151919 、授权给 Dent 等人的美国专利 5353352 以及 1993 年 11 月 22 日提交的美国专利申请 08/155557 。

发明概要

根据本申请人的发明，无线电信道的特性被用来几乎完善保密地建立和交换密钥。这些特性是无线电信道的相位的短期互易性和迅速的空间解相关。换句话说，对于一段短的时间（几微秒的数量级），从位置A的天线看到位置B的天线的无线电信道的脉冲响应与从位置B看到位置A的信道的脉冲响应相同，但不包括热噪声。可以利用等效于一种有界距离译码过程的计算来建立密钥，可用一个用来建立密钥的译码器来处理随后的数据传输。

因此，与传统的密码系统和 PKC 密码系统相比，本申请人的发明提供了建立和共享一种依赖于物理过程的密钥的替代机制。在申请人的系统中，由于通信信道本身的时间和空间上的非平稳性提供了必需的随机性，所以每一方都不需要产生伪随机数。通过利用信道译码器，两个用户建立相同密钥的概率接近1，而窃听者建立该同一密钥的概率基本上是0。这称为“概率保密”。还有，可能的密钥的数目足够大，以致利用穷举搜索找出正确密钥是不实际的。这称为“计算保密”。这些概率测度不同于 Shannon（仙农）的完备机密测度。

在一个方面中，申请人的发明提供了一种建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的方法，该方法包括以下步骤：在第一无线电收发信机中，发送多个正弦波信号，每一正弦波信号具有各自预定的频率和预定的初始相位；在第二无线电收发信机中，检测第一无线电收发信机发送的这些正弦波信号，并在预定时间周期后发送这些多个正弦波信号。该方法还包括以下步骤：在第一和第二无线电收发信机的每一个中，确定从对方无线电收发信机所接收的多个正弦波信号的每一个的相位；确定所接收的各对正弦波信号的相位之间的差值；把每一差值量化成为多个相位判决值中相应的一个；以及按照预定的分组码把多个量化差值译码成为一个密钥序列。

该方法还可以包括确定多个正弦波信号的每一个的振幅的步骤，其中，这些振幅在译码步骤中被用作软信息。该方法还可以包括在第一和第二无线电收发信机的至少一个中根据密钥序列加密待发送信息的步骤；以及在第一和第二无线电收发信机的至少另一个中根据密钥序列解密所加密的发送信息的步骤。

在另一个方面中，申请人的发明提供了建立供第一无线电收发信机

和第二无线电收发信机之间的安全通信用的密钥序列的方法，该方法包括以下步骤：在第一无线电收发信机中，发送包括多个比特的预定数字字；在第二无线电收发信机中，检测第一无线电收发信机发送的该预定数字字，并在预定时间周期后发送该预定数字字。该方法还包括以下步骤：在第一和第二无线电收发信机的每一个中，对于从对方无线电收发信机所接收的预定数字字的多个比特中的每一个比特进行硬判决译码；以及按照预定的分组码把硬判决译码的这些比特变换成为密钥序列。

在另一个方面中，申请人的发明提供了建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的方法，该方法包括以下步骤：在第一无线电收发信机中，发送包括多个比特的预定数字字；在第二无线电收发信机中，检测第一无线电收发信机所发送的该预定数字字，并在预定时间周期后发送该预定数字字。该方法还包括以下步骤：在第一和第二无线电收发信机的每一个中，确定从对方无线电收发信机所接收的多个比特中的每一个比特的相位；确定被确定的每一相位和相应的预定相位之间的差值；把每一差值量化成为多个相位判决值中相应的一个；以及按照预定的分组码把多个量化差值译码成为密钥序列。

在其它各个方面中，申请人的发明提供了建立供第一无线电收发信机和第二无线电收发信机之间的安全通信用的密钥序列的几种设备。

附图概述

以下参照仅作为例子给出的、结合附图说明的实施例，更详细地描述申请人的发明，图中：

图 1A、1B 表示示范性多层蜂窝系统；

图 2A ~ 2C 表示示范性时隙格式；

图 3 是示范性蜂窝移动无线电话系统的方框图；

图 4 是表示一通信系统的方框图；

图 5 是表示利用单音梳（comb of tones）建立密钥序列的通信系统的方框图；

图 6 表示相位空间判决区域；

图 7 表示随机变量ψ的概率密度函数；

图 8 是利用导引符号建立密钥序列的通信系统的方框图；

图9表示根据申请人的发明的通信系统的性能。

详细描述

虽然以下的描述在涉及到便携或移动无线电电话和/或个人通信网络的蜂窝通信系统的范围内，但本领域的普通技术人员都懂得申请人的发明可用于其它通信应用。

系统综述

考虑由具有被包含在 Galois 域（有限域）GF（$M = 2^m$）内各元的所有矢量、即所有 $\mathbf{r}=(r_1,r_2,\cdots,r_n)$、其中 $r_i \in GF(M=2^m)$组成的 n 维矢量空间。（以下矢量或序列用黑体来表示，而标量和函数用普通体来表示。）对于某一汉明半径 t，M^n 个矢量 **r** 就是被装入 S 个球内的 t-球，即半径为 t 的不相交球的最大数目是 S。一球内的矢量被变换成为包括该球的中心的一代表矢量。令 S 个代表矢量的集合是$\{\mathbf{c}_1,\mathbf{c}_2,\cdots,\mathbf{c}_s\}$。每一代表矢量 $\mathbf{c}_i$ 的长度是 n，可被变换成为长度为 mn 的一个二进制矢量 **k**。令相应的二进制矢量的集合是 $\mathbf{K}=\{\mathbf{k}_1,\mathbf{k}_2,\cdots,\mathbf{k}_s\}$。

如果发射机和接收机能够以大的概率建立被包括在集合 **K** 内的一公共序列 $\mathbf{k}_i$，则可用该序列 $\mathbf{k}_i$ 来扩展从发射机传送给接收机的信息序列。此外，如果窃听者能够确定该公共序列 $\mathbf{k}_i$ 的概率基本上是 0，则还实现了安全通信—没有采用额外的加密和解密算法来实现密码的安全保密性。

按照申请人的发明构造的球提高了发射机和接收机在无线电信道和系统硬件存在噪声和其它差异的情况下建立这种公共序列 $\mathbf{k}_i$ 的概率。一般来说，发射机建立序列 $\mathbf{r}_T$ 而接收机建立不同的序列 $\mathbf{r}_R$。如果序列 $\mathbf{r}_T$、$\mathbf{r}_R$ 落在同一球内，它们就将被变换成为集合 **K** 内的同一序列 **k**。

因此，申请人的发明提供了建立两个序列（一个在发射机处而另一个在接收机处）从而使这两个序列以大的概率落在同一球内的方法和设备。此外，这两个序列不在同一球内的罕见事件可迅速检测，使得建立公共序列的过程可被重复。这样，以实时和低的硬件复杂性有效地确定了与一任意矢量相关的球。

序列建立

广义的通信链路包括两个通信信道：从第一用户的发射机至第二用户的接收机的信道和从第二用户的发射机至第一用户的接收机的信

道。人们可以认为该链路包括到达希望获取第一和第二用户交换的信息的窃听者的第三信道。这种简单情况如图 4 所示，该图表示第一用户 A、第二用户 B 和窃听者 E。一般来说，AB 信道、BA 信道和 AE 信道的特性都随时间变化。每一信道中的热噪声用加性噪声项 ni(t)来表示，其中 i=1,2,3。

虽然它们随时间变化，但在不考虑热噪声时，A－B 信道的脉冲响应与 B－A 信道的脉冲响应相同，即在一段短的时间周期内，其数量级为几毫秒，该链路是互易的。应当知道在包括热噪声（和其它可能的非理想状态）时，该链路就不是互易的。

此外，了解以下事实也是重要的，即 A－B 信道和 B－A 信道的脉冲响应与第一用户－窃听者的 A－E 信道和第二用户－窃听者的 B－E 信道的脉冲响应不相同。这种不同是因信号相位与变化的空间位置迅速地解相关而造成的。

以下描述建立密钥序列的两种方法。

单音梳

以下紧接的描述涉及每次两个单音的传输，但应当懂得，如后面所描述的，每次也可以发送两个以上的单音。

参看图 5，假定第一收发信机、例如第一用户 A 在第 k 个信号间隔[kT,(k+1)T]期间发送包括两个正弦波的信号 s(t)，这两个正弦波的频率是 f_1 和 f_2，具有相同的初始相位偏移 ϕ 和能量 E。可以按照若干种方式中的任一种方式产生发送信号 s(t)，例如放大和求和两个合适的振荡器 501、503 或一频率合成器的输出信号，以及通过调制一载波信号把放大和求和的结果上变频成为合适的传输频率。不考虑调制，则发送信号 s(t)用以下公式来表示：

$$s(t) = \sqrt{2E/T}\cos(2\pi f_1 t + \phi) + \sqrt{2E/T}\cos(2\pi f_2 t + \phi) \qquad \text{（公式 1）}$$

一般来说，发送信号 s(t)利用天线进行发射，通过例如空气这样的信道，这种信道通过引入因多径传播造成的时变衰落和通过增加具有双边带功率谱密度 $N_0/2$ 的白高斯噪声 n(t)而使发送信号发生变化。

接收机把其从信道获得的信号进行下变频和放大（下变频器和放大器在图 5 中未示出），并使由此形成的信号 r(t)与接收机自己本地产生

的 cos（ $2\pi f_1 t$ ）和 cos（ $2\pi f_2 t$ ）相关。如图 5 所示，虽然许多其它为本领域普通技术人员熟知的装置可以使用，但每一相关可以利用合适的混频器 505、507 和可复位积分器 509、511 来实现，积分器在连续的时间间隔 $T = 1/2\pi f_i$ 期间积分混频器的输出信号。相关器产生的输出信号被低通滤波器 513、515 进行常规的滤波，以便抑制和（上变频）信号以及由邻近无线电信号产生的分量。

假定正弦波 cos（ $2\pi f_1 t$ ）和 cos（ $2\pi f_2 t$ ）是正交的并至少被间隔开信道的相干带宽，则第三收发信机、例如第二用户 B 在第 k 个信号间隔期间接收的信号 r(t)可用下式给出：

$$r(t) = \sqrt{2\Lambda_1^2(k)E/T}\cos(2\pi f_1 t + \theta_1(k)) + \sqrt{2\Lambda_2^2(k)E/T}\cos(2\pi f_2 t + \theta_2(k)) + n(t)$$

其中振幅系数$\Lambda_i(k)$， i=1,2 是相同分布的独立随机变量。

对于受瑞利分布衰落影响的信道，变量$\Lambda_i(k)$具有由下式给出的瑞利概率密度：

$$p_A(\lambda_i) = \begin{cases} \frac{\lambda_i}{\sigma^2}\exp(-\frac{\lambda_i^2}{2\sigma^2}), \text{ for } \lambda_i \geq 0 \\ 0, \qquad \text{for } \lambda_i < 0 \end{cases} \qquad \text{（公式 2）}$$

其中$\sigma^2 = E\{\Lambda^2_i(k)\}$是信道的特性，$E\{.\}$表示关于 P_A 的期望值。相位项$\theta_1(k)$和$\theta_2(k)$是相互独立的随机变量，每个具有在区间$[-\pi,\pi]$内为均匀的概率密度。

对于具有其它特性、例如 Rician 分布衰落的通信信道可以求出接收信号 r(t)的类似表达式。例如，Rician 分布信道的概率密度由下式给出：

$$p_A(\lambda_i) = \begin{cases} \frac{\lambda_i}{\sigma^2}\exp(-\frac{\lambda_i^2 + s^2}{2\sigma^2})\, I_0(\frac{\lambda_i s}{\sigma^2}), \text{ for } \lambda_i \geq 0 \\ 0, \qquad \text{for } \lambda_i < 0 \end{cases} \qquad \text{（公式 3）}$$

其中 I_0（.）是零阶的修正贝塞尔函数，而 s^2 是直接视距分量的功率。

在第二用户 B 的收发信机中，将滤波的相关器输出信号提供给差分

相位检测器 517，对于每一时间间隔 T，该差分相位检测器 517 产生相位项$\theta_1(k)$和$\theta_2(k)$之间差值的估算值。逐次的相位差估算值被提供给量化器 519，该量化器 519 给每一相位差估算值分配若干个预定相位值中相应的一个相位值。根据申请人的发明，只要求不同时间间隔的相位差估算值彼此不相关。（以下在不引起歧义的情况下将省略时标 k。）

由接收机 B 内的差分相位检测器 517 产生的基带差分信号由以下公式给出：

$$U_B = 2\Lambda_1\Lambda_2 E\exp[j(\Theta_1 - \Theta_2)] + \Lambda_1 N_1 + \Lambda_2 N_2^* = X_B + jY_B \qquad \text{（公式 4）}$$

其中 N_1 和 N_2 是具有零平均值和方差 $\sigma^2 = 2EN_0$ 的复值高斯随机变量，“*”表示共轭。相位差估算值由 $\Phi^B = \tan^{-1}Y_B/X_B$ 给出。如上所述，第二用户 B 把该相位差估算值量化成为 M 个预定相位值之一，产生量化器输出信号 $Q(\Phi^B)$，图 6 表示 M = 4 的相位空间判决区域。

差分相位检测器或相位测量装置 517 可以产生基带信号的瞬时相位的模拟或数字测量结果。合适的差分检测器是在 Dent 的美国专利 5084669 号和 Holmqvist 的美国专利 5220275 号中所描述的相位检测器的两个的组合，在此特意把这两份美国专利作为参考文献。

通过在每一时间 k=1，2，…，n 重复上述估算－量化过程，第二用户 B 就建立了由下式给出的量化相位差估算值的序列：

$$r_B = [\,Q(\Phi_1^B),\ Q(\Phi_2^B),\ \ldots,\ Q(\Phi_n^B)\,]. \qquad \text{（公式 5）}$$

将量化器 519 所产生的各相位值的这一序列 $\mathbf{r_B}$ 存储在诸如随机存取存储器、移位寄存器或等效装置一类的缓冲器 521 内，该缓冲器 521 的长度由最小距离纠错译码器 523 的各参数来确定。接收机 B 内的纠错译码器 523 变换量化相位差估算值的序列，并产生相应于接收机的密钥序列 $\mathbf{k_B}$ 的输出信号。

实际上，缓冲器 521 的大小由所需密钥序列的长度来确定。如果译码器 523 具有码组长度 N 和维数 k，则对于单音梳只包括在 N 个时刻的每一时刻被同时传送的两个单音的这一例子，缓冲器延迟是 N。如下所

述，可同时传送两个以上单音，这样就相应地缩短了缓冲器延迟。例如，如果 T 个单音被同时传送，则每次就能够量化 T - 1 个相位差，缓冲器延迟就是 N/(T-1)。

缓冲器 521 所产生的矢量 $\mathbf{r}_B$ 具有 N 个元素，每一元素有 M 个状态（ M - ary ），该 N 元素矢量是任一个种类繁多的最小距离译码器 523 的输入。一种有用的译码器是有界距离译码器（ bounded distance decoder ），它是位于麻萨诸塞州 Reading 的 Addison-Wesley 于 1983 年出版的 R. Blahut 所著的《差错控制码的理论和实践》第 7 章中所描述的低复杂性译码器。如以下所详述的，译码器 523 将缓冲器产生的 N 个符号变换成为另外的 N 个符号，这另外的 N 个符号就是感兴趣的密钥序列 $\mathbf{k}_B$。

可以看出在接收机中所执行的信号处理操作可以利用合适的数字信号处理（ DSP ）装置在数字域中来进行。利用这种结构，通过把 DSP 装置编程成为能够恰当地处理接收信号的数字样值，就能够检测几乎任何类型的调制，例如在 Dent 等人的题目为“多方式信号处理”的美国专利申请 07/967027 中所描述的，在此特意把该美国专利申请作为参考文献。应当懂得可以把 DSP 装置设计成为硬布线逻辑电路，或者最好设计成为集成数字信号处理器，例如专用集成电路（ ASIC ）。当然，也应懂得 ASIC 可以包括能够最有效地完成所需功能的硬布线逻辑电路，这是当速度或另外的性能参数比可编程数字信号处理器的通用性更重要时通常选择的电路结构。

按照类似于上述的方式和利用类似于上述的硬件，第一用户 A 根据第二用户 B 发送的信号建立其自己的量化相位差估算值的序列。在第一用户传输后的延迟可忽略的情况下，即延迟比信道的相干带宽小的情况下，第二用户 B 发送包括两个正弦波的信号，这两个正弦波的频率是 f_1 和 f_2，并具有相同的相位偏移和能量。换句话说，以交错的方式，第一用户 A 发送，而后是第二用户 B，然后是第一用户 A，如此进行下去，以便保证互易性假定。

假定第一用户 A 是相对于基站或其它收发信机（第二用户 B ）以 100 公里/小时的速度运动的无线电话，使用 900MHz 频段的射频载波，如果第一用户进行的发送和第二用户进行的发送之间的延迟是 10 微秒，则无线电话在每一延迟期间仅移动 0.28 毫米，该距离与 0.3 米的波

长相比是可忽略的。因此，来自各个反射物的信号散射应当是强相关的。还有， 10 微秒的延迟比因多径传播造成的所有信号射线都到达第二用户通常所需的时间长，比保证信道的互易性所需的几个毫秒短。如果运动更慢或延迟更短，信道的互易性就更加精确。

于是第一用户 A 产生由下式给出的基带差分信号（它自己的差分相位检测器的输出）：

$$U_A = 2\Lambda_1\Lambda_2 E \exp[j(\Theta_1 - \Theta_2)] + \Lambda_1 V_1 + \Lambda_2 V_2^* = X_A + jY_A \qquad \text{（公式 6）}$$

其中 V_1 和 V_2 与 N_1 和 N_2 无关。第一用户 A 产生的估算相位差是 $\Phi^A = \tan^{-1}Y_A/X_A$。可以看出，由于信道的互易性， U_A 和 U_B 之间唯一的差别是加性高斯噪声。

通过依次重复估算－量化过程，第一用户 A 就建立了由下式给出的相位差估算值的序列：

$$r_A = [\ Q(\hat{\Phi_1}),\ Q(\hat{\Phi_2}),\ \ldots,\ Q(\hat{\Phi_n})\ ]. \qquad \text{（公式 7）}$$

该序列存储在第一用户的收发信机的缓冲器内并提供给该第一收发信机的相应纠错译码器。

根据这些发送信号，窃听者 E 能够获得由下式给出的基带差分信号：

$$U_E = 2\Lambda_3\Lambda_4 E \exp[j(\Theta_3 - \Theta_4)] + \Lambda_3 V_3 + \Lambda_4 V_4^* = X_E + jY_E \qquad \text{（公式 8）}$$

其中 Λ_i， i=1,2,3,4 是相互独立的。窃听者的估算相位差是 $\Phi_E = \tan^{-1}Y_E/X_E$。还有， θ_i， i=1,2,3,4 是相互独立的随机变量。窃听者 E 能够建立由下式给出的相位差估算值的序列：

$$r_E = [\ Q(\Phi_1^E),\ Q(\Phi_2^E),\ \ldots,\ Q(\Phi_M^E)\ ] \qquad \text{（公式 9）}$$

如上所述，所建立的三个序列或矢量 $\mathbf{r}_A$、$\mathbf{r}_B$ 和 $\mathbf{r}_E$ 的每一个作为输入信号提供给相应的纠错译码器。这些译码器产生的输出信号相应于密钥序列 $\mathbf{k}_A$、$\mathbf{k}_B$、$\mathbf{k}_E$。应当指出在发射机 A、B 处不需要执行加密。如以下更详细描述的那样，译码器限制可能的密钥的数目来提高第一用户和第二用户建立相同密钥的概率。

为了说明为什么单音 f_1、f_2 必需具有间隔足够宽的频率以便它们的相位是独立的，令

$$\psi \triangleq (\theta_1 - \theta_2) - (\theta_3 - \theta_4). \qquad \text{（公式 10）}$$

并定义

$$g(x) = \frac{1-\alpha^2}{4\pi^2}\frac{\sqrt{1-\alpha^2\cos^2 x} + \alpha\cos x\,\cos^{-1}(-\alpha\cos x)}{(1-\alpha^2\cos^2 x)^{3/2}} \qquad \text{（公式 11）}$$

其中 $\alpha^2=J_0^2(\omega_D\tau)/[1+(\omega_1-\omega_2)^2\sigma^2]$；$J_0$ 是零阶贝塞尔函数；ω_D 是发射机和接收机之间的相对运动造成的多普勒频移；τ 是传输时延；σ 是多径信号射线之间的时延扩散。则如在 John Wiley & Sons 于 1974 年出版的小 W. C. Jakes 编辑的《微波移动通信》第 1 章中所描述的，ψ 是具有由下式给出的概率密度函数的随机变量：

$$p_\psi(\psi) = 4\pi^2 \int_0^\pi g(x)[g(x+\psi) + g(x-\psi)]\,dx \qquad \text{（公式 12）}$$

图 7 表示对于参数 α^2 的 5 个不同的值，作为 ψ/π 的函数的概率密度函数 p_ψ。对于 40KHz 的频率间隔（$\omega_1-\omega_2$）和 5 微秒的时延扩散 σ（就是说，即使对于 $\omega_D\tau=0$ 的最坏情况，$\alpha^2<0.4$），随机变量 ψ 几乎是均匀分布的。在这种情况下，量化器以等概率 1/M 把相位差估算值量化成为 M 个相位值中的每一个相位值。系统的保密性取决于通过通信信道时单音的相位被解相关的程度。如果解相关基本上是完全的，则窃听者破译系统所必需做的工作量就接近对密钥序列 $\mathbf{k}_A$、$\mathbf{k}_B$ 进行穷举搜索的工作量。

应当认识到，以上的分析因假定两个单音具有相等的能量和相等的初始相位偏移而得到简化，例如，相等的能量和相等的初始相位偏移可

利用锁相环容易地获得。一般来说，这些参数只需要是预先被确定的，即预先为两个收发信机所了解，但这样的系统比上述系统复杂。

还有，以上的分析只考虑了在任一时刻被发射的两个单音，但一般来说，单音梳可以由两个以上同时被发送的单音组成，以上的分析适用于多对接连的这种单音梳。事实上，通过同时发送具有恰当个数单音的单音梳，并对每一接连的单音对的相位差进行估算和量化，就能够同时产生序列 $\mathbf{r_A}$、$\mathbf{r_B}$。因为同时发送两个或更多的单音可以容易地控制这些单音的初始相位，使系统不那么复杂，所以希望同时发送两个或更多的单音。

此外，一对单音的单音之间的频率分隔不必与另一对之间的频率分隔一样；换句话说，“单音梳”可以具有间隔不均匀的“齿”。也不必只考虑接连单音的对；换句话说，一对中的“齿”可以被其它“齿”隔开。例如，如果单音梳包括按递增频率顺序排列的 10 个单音 f_1，f_2，…，f_{10}，则随机变量ψ 的必需的均匀分布（见图 12）可以通过诸如单音 f_1 和 f_4、f_2 和 f_5、f_3 和 f_6 等的配对来获得。每对中的单音只需要被正交地隔开，即频率分隔必需是如上所述地足够宽。

引导符号

除如上所述地发送正弦波梳外，还可以只根据多个引导符号、例如可以发送用以同步第一收发信机和第二收发信机的操作的各比特来建立密钥序列 $\mathbf{k_A}$、$\mathbf{k_B}$。这种同步比特一般被包括在以上参看图 2A - 2C 描述的普通蜂窝无线电话系统内。以下描述根据引导符号建立密钥的两种方法。

通过对引导符号进行硬判决译码和把所得到的译码引导符号序列映射至球的中心就可粗略地建立序列 $\mathbf{k}$。可以认为，第一用户译码的序列中的任何差错与第二用户译码的序列中的差错一样。因此，两个引导符号序列将被映射至同一个球，产生相同的密钥。即使第一和第二用户译码的序列中的差错略微不同，这两个序列将仍被以高的概率映射至同一个球，产生相同的密钥。这一方法的可能的不足在于，需要许多引导符号来使窃听者在计算上难于穷举所有的可能性。如果引导符号是蜂窝无线电话系统内的同步比特，目前认为至少需要 60 个比特。

应当认识到，所须的引导符号无需一起被发送，就是说，不必在 TDMA 信道的一个时隙内使用所有的同步比特。例如，一个时隙内的任

何一个或多个同步比特可以与其它时隙内的任何一个或多个同步比特一起被使用。如上所述，只要求将各时隙以比信道的相干时间长的时间间隔进行分隔。

根据引导符号建立密钥序列的严密方法是利用信道状态信息而不是利用硬判决译码。在这一方法中，第一和第二用户按照类似于以上对于根据单音梳建立密钥的方法所描述的方式内插已知的引导符号和量化内插器的输出。

例如，在必要时对所接收信号进行了下变频、放大和滤波之后，第二用户确定时隙同步部分的每一个比特的相位估算值。当然，第一和第二用户可以一致同意利用另一组已知的比特。第二用户确定每一相位估算值和已知比特的各个预定相位之间的差值。如以上对于利用发送单音梳的密钥建立所描述的那样，这些相位差估算值然后被量化并提供给最小距离译码器。

图 8 是实现这一利用引导符号的“严密方法”的系统的方框图。在第一收发信机中，待发送数据被加密器 801 根据密钥序列进行加密。当然，在密钥序列被建立之前，该加密器将仅仅传送待发送数据而不作任何改变。多路复用器 803 把被加密的待发送数据与已知引导符号组合，这些已知引导符号可以是在普通无线电话中用于同步和开销信令的比特。只要求待发送引导符号具有已知的相位。多路复用器 803 所形成的数据和引导符号交织的序列被提供给脉冲成形器和上变频器 805，以便通过通信信道发送该信息，该通信信道一般用衰落和加性白高斯噪声来表征。

在进行接收的第二收发信机处，将从信道所接收的信号进行必需的下变频，并经由匹配滤波器 807 进行传送，将匹配滤波器 807 产生的信号用恰当控制的开关 809 或抽取器分成一个包括所收到的被发送的数据的信号和一个包括所接收的引导符号的信号，内插器 811 测量所接收引导符号的相位，产生通常已被信道衰落改变了的每一测量相位和各个引导符号的已知发送相位之间的差值。内插器 811 最好低通滤波这些相位差估算值。内插器 811 产生的这些相位差值被量化器 813 量化，如果需要的话，存储在缓冲器 815 内以便累积足够的相位差值，然后被译码器 817 译码，以便如以上参看图 5 所描述的那样产生密钥序列。

内插器 811 产生的相位差值还提供给例如纠错译码器这样的解调器

819，以便恢复被发送的数据。解调器 819 还接收被发送的数据，这些被发送的数据可能已通过了适合于同步相位差值和被发送数据的延迟装置 821。假定所接收数据在传输之前被按照密钥序列进行了加密，则解调器 819 产生的加密发送数据和译码器 817 产生的密钥序列就提供给解密器 823，以便恢复被发送的数据。

按照类似于上述的方式和利用类似于上述的硬件，发射机就根据来自接收机的传输建立了其自己的密钥序列，该密钥序列可用来解密来自接收机的加密传输。

球封装和联合

假定 **K** 是给定的并且球是预先确定的，则把一任意序列映射至一个球的一般问题是 NP 费力的（ NP-hard ），就是说，该问题的计算复杂性与可能的球的数目成正比。对于安全传输和扩展的这种应用，球的数目过大。尽管如此，把一简化结构用于候选序列 **k**（相应于球的表示 **c**）将起到将计算复杂性减轻到可接受程度的作用。

根据申请人的发明，候选序列的集合被限制为线性纠错码序列的集合。球的半径于是由代码的纠错能力、即该代码能够校正的差错的数目来确定，并可利用合适的已知译码过程将所接收的序列 **r** 变换成为候选序列 **k**。

作为一个具体的例子，线性 Bose-Chaudhuri-Hocquenghem （ BCH ）码可用作候选序列 **k** 的集合；如在以上引用的 R. Blahut 的书中所描述的那样，可利用 Peterson-Gorenstein-Zierler 过程、 Berlekamp-Massey 过程或译码循环码的任何过程简单地译码这种码。如果码参数是（ n,k ），最小汉明距离是 d，码符号字母表是 GF （ 2^m ），就可以根据大小为 2^{mn} 的集合建立长度为 mn 的候选序列。球的汉明半径 t 或等效的码纠错能力由 $t \le [(d-1)/2]$ 来给出。（球不必紧密地封装）。

所接收的序列 $\mathbf{r}_A$、 $\mathbf{r}_B$ 和 $\mathbf{r}_E$ 都是执行 Berlekamp - Massey 过程的纠错译码器的输入。这些译码器的输出是序列 $\mathbf{k}_A$、 $\mathbf{k}_B$ 和 $\mathbf{k}_E$。还应注意到发射机不需要进行加密。译码器显著地限制了可能序列的数目，由此提高了第一和第二用户之间序列一致的似然性。应当指出，在这种非常高的信噪比（ SNR ）的情况下可以不需要译码器，不过在实际的通信系统中难于获得非常高的信噪比（ SNR ）。

在许多通信系统中，对要发送的信息序列进行分组编码来纠错。在

正交分组编码中， N 个信息比特被变换成为 2^N 个 N 比特正交码字之一。译码这种正交码字需要使其与 2^N 个码字集合的所有元相关。给出最大相关的码字的二进制相关指数将给出所需的信息。例如，如果所接收的 16 比特码字与具有指数 0 - 15 的 16 个正交 16 比特码字的集合中的每一个的相关性在第 10 个码字上形成最大的相关性，则优先的信息信号就是 4 位二进制码字 1010（它是十进制表示的整数 10）。这种代码被称为[16,4]正交分组码。通过倒置码字的所有位，则每一码字还可以传送另一个位的信息。这种编码被称为双正交分组编码。这种编码的一个显著特点是可以利用“快速沃尔什变换”（ FWT ）装置有效地实现与一集合中的所有正交分组码字的同时相关。例如在[128,7]分组码的情况下， 128 个输入信号样值被变换成为 128 点的沃尔什频谱，该频谱中的每个点代表这些输入信号样值与集合中的码字之一相关的值。在此作为参考文献的 Dent 的美国专利 5357454 描述了一种合适的 FWT 处理器。

性能分析

为了评定申请人的序列一致系统的性能，假定以下事件是有用的:

$$G_i = \{\Theta_A \in R_i,\ \Theta_B \in R_i\}, \quad B_i = \{\Theta_A \in R_i,\ \Theta_E \in R_i\}.$$

第一和第二用户之间符号一致的概率用下式来表示:

$$P_g = Pr\left\{\bigcup_{i=1}^{M} Pr(G_i)\right\} = \sum_{i=1}^{M} [Pr\ (\Theta_A \in R_i)]^2 \qquad \text{（公式 13）}$$

第一用户和窃听者之间符号一致的概率用下式来表示:

$$P_b = Pr\left\{\bigcup_{i=1}^{M} Pr(B_i)\right\} = \frac{1}{M} \qquad \text{（公式 14）}$$

判决区域内的估算相位θ 的概率密度函数可如下地求出。首先假定$\Delta = \theta_1 - \theta_2$是已知的，且等于零。考虑到如下情况:

给Λ_1和Λ_2加上条件，即 $E\{X\} = 2\Lambda_1\Lambda_2 E\underline{\Delta}\mu$； E（ y ）= 0；方差（ X ）= 方差（ Y ）= $2EN_0\ (\Lambda_1^2 + \Lambda_2^2)\ \underline{\Delta}\sigma_0^2$。

$$U = 2\Lambda_1\Lambda_2 E + \Lambda_1 N_1 + \Lambda_2 N_2^*$$
$$= X + jY$$
$$X = 2\Lambda_1\Lambda_2 E + Re(\Lambda_1 N_1 + \Lambda_2 N_2^*)$$
$$Y = Im(\Lambda_1 N_1 + \Lambda_2 N_2^*)$$

x 和 y 的条件联合概率密度函数用下式来表示:

$$p(x,y|\Lambda_1,\Lambda_2) = \frac{1}{2\pi\sigma_0^2}\exp\left\{-\left[(x-\mu)^2 + y^2\right]/2\sigma_0^2\right\}$$

变量的变化是:

$$R = \sqrt{X^2 + Y^2},\ and\ \theta = \tan^{-1}\frac{Y}{X}$$

θ 和 R 的条件联合概率密度函数用下式来表示:

$$p(r,\theta|\Lambda_1,\Lambda_2) = \frac{r}{2\pi\sigma_0^2}\exp\left\{-\left(r^2 + \mu^2 - 2\mu r\cos\theta\right)/2\sigma_0^2\right\}$$

在区间 r∈[0,∞]内积分，则θ 的概率密度函数可表示如下:

$$p_\theta(\theta|\Gamma) = \frac{1}{2\pi}\exp(-\Gamma)$$

$$+\frac{1}{\sqrt{2\pi}}\left(\sqrt{\Gamma}\cos\theta\right)\exp\left(-\Gamma\sin^2\theta\right)\left[1 - Q\left(\sqrt{2\Gamma}\cos\theta\right)\right]$$

其中，

可以证明Δ′在区间[－π，π]内是均匀分布的。在由 R_i=[-πi/M, πi/M] 给定的区域内，i = 1，…，M，则判决区域内的估算相位θ 的所需概率是:

$$\Gamma = \frac{\Lambda_1^2\Lambda_2^2}{\Lambda_1^2 + \Lambda_2^2}\frac{E}{N_0}$$

$$Pr(\theta \in R_i) = \frac{1}{2\pi}\int_0^\infty\int_{-\pi}^{\pi}\int_{R_i} p_\theta(\theta - \delta|\Gamma)\,P(\Gamma)\,d\theta\,d\delta\,d\Gamma$$

现在考虑具有最小汉明距离 d、维 **k** 和码组长度 n 的线性分组码的使用。设 t = [(d-1)/2]为译码器能够校正的差错的个数。第一和第二用户建立的序列一致的概率就是两个接收矢量位于码字的同一译码区域内的概率。

译 C 是汉明权重为 l 的码字。有三个矢量 **c**、$\mathbf{r}_A$ 和 $\mathbf{r}_B$ 为变量。重新排列这些矢量的坐标不会改变性能分析。一种这样的排列如下:

$$\mathbf{c} = \overbrace{1111111 \ \ldots \ 11111}^{l} \ \overbrace{0000000 \ \ldots \ 00000}^{n-l}$$

$$\mathbf{r}_a = \overbrace{111 \ \ldots \ 11}^{H} \ \overbrace{000 \ \ldots \ 00}^{j} \ \overbrace{111 \ \ldots \ 11}^{k} \ \overbrace{000 \ \ldots \ 00}^{n-l-k}$$

$$\mathbf{r}_b = \overbrace{1\ldots1}^{H-m_1} \overbrace{00..0}^{m_1} \overbrace{11\ldots1}^{m_2} \overbrace{00..0}^{j-m_2} \overbrace{11\ldots1}^{k-m_3} \overbrace{00\ldots0}^{m_3} \overbrace{111..1}^{m_4} \overbrace{00\ldots0}^{n-k-l+m_4}$$

可以证明: 序列一致和该序列是 **c** 的概率可用下式来表示:

$$P_l = \sum_{j=0}^{l} \sum_{k=0}^{n-1} \sum_{m_1=0}^{l-j} \sum_{m_2=0}^{j} \sum_{m_3=0}^{k} \sum_{m_4=0}^{n-l-k} \begin{bmatrix} n \\ \beta \end{bmatrix} (1-p_s)^{\beta} p_s^{n-\beta} \qquad \text{(公式 15)}$$

其中:

$$\beta = m_1 + m_2 + m_3 + m_4$$

$$0 \le j + k \le l$$

$$0 \le m_1 + j - m_2 + k - m_3 + m_4 \le l$$

因此，相互一致的概率是:

$$Pr(k_A = k_B) = \sum_l A_l P_l$$

其中 A_l 是码的权重计算器函数。窃听者建立的序列一致的概率 P_B 由用 P_b 代替 Pg 的相同方程来给出。在不用译码器的条件下，则 Pr（ $\mathbf{k_A}=\mathbf{k_B}$ ）= Pr（ $\mathbf{r_A}=\mathbf{r_B}$ ）$=P_g^n$， Pr（ $\mathbf{k_A}=\mathbf{k_E}$ ）= Pr（ $\mathbf{r_A}=\mathbf{r_E}$ ）$=1/M^n$。

讨论在这种序列一致系统中所涉及的折衷是重要的。小值的维 k 导致具有良好的纠错能力的码，但随着 k 的减小，可以实现的穷举搜索的速度指数地增大。由于码限制了备选序列空间的大小，所以码参数的选

择是至关重要的，但减小不应导致不安全的系统。

对于判决区域的大数 M，可以采用较大的码，这样就增大了系统的计算保密性；同样地，P_b 减小，导致良好的概率保密性。但是，这不足以获得良好的密码系统。由于增大的 M，热噪声影响变成主要的，需要增大 E_b/No（比特能量与噪声能量之比）来实现具有与一定的概率保密性的序列一致。因此，在计算保密性、概率保密性和发送能量之间存在折衷。

作为另一个例子，考虑在 GF（32）范围内的（31，13）里德－所罗门码的应用。码的大小（可能的码字、即比特序列的个数）是 $32^{13} = 2^{65}$，计算保密性显著地优于 DES 2^{56} 的计算保密性，DES 2^{56} 是采用数字加密标准的系统的序列，包括 56 个保密比特和 8 个奇偶校验比特。这种里德－所罗门码的最小汉明距离是 18。

图 9 表示采用这种里德－所罗门码的安全通信系统的性能。还示出了（61，11）里德－所罗门码的性能以及两个未编码系统的性能。从图 9 可以看出，在使用信道译码器的情况下，在 M = 64 和 M = 32，信噪比 E_b/Eo 分别为 11dB 和 13dB 的情况下，第一和第二用户建立的密钥不一致的概率为 10^{-8}，与没有译码器的通信系统相比，这分别是约 9dB 和 4dB 的增益。此外，Pr（$\mathbf{k_A}=\mathbf{k_B}$）≈0，Pr（$\mathbf{r_A}=\mathbf{r_E}$）≈0（两者都约为 10^{-41}）。

在这种系统中，虽然如上所述不是严格的要求，但第一和第二用户最好是使用译码器，但译码器的使用对窃听者没有帮助。为了扩展所发送信息或解扩展所接收信息，可以按原样地使用译码器所产生的序列，或者可以使用该序列的全部或部分的二进制表示。应当注意到，这一“扩展”不是指在 CDMA 系统中执行的扩展。虽然根据申请人的发明建立的密钥序列可用来加密和解密在 CDMA 系统中传送的信息，但由于这些序列的不受控制的互相关特性，所以申请人的密钥序列通常不适合用作 CDMA 扩展序列。

申请人的基于无线电信道的可逆性的序列一致方法和设备提供了优异的计算保密性和概率保密性。利用申请人的发明，能够共享任意长的密钥，并且，即使在通信的“对话”期间也能够改变密钥序列。在蜂窝无线电话系统中，至少每当移动台在通信系统中进行登记时希望建立新的密钥序列，甚至可能更频繁地，例如对于每一呼叫或每当预定的时

间间隔满时后就建立一个新的密钥序列。

不使用线性分组码，安全通信系统可以使用每一用户发送的 2M 个正交单音的单音梳。这种单音梳系统具有与分组码系统相同的性能，但如正交信号所要求的那样，单音梳系统需要大得多的带宽，以及用来产生这些单音的更复杂的频率合成器。

在任一系统中，安全性的性能测度是概率测度，并且不同于完善保密的仙农测度。尤其在分组码系统中，两个用户建立相同密钥序列的概率接近 1，而窃听者建立相同序列的概率基本上是零。这就是概率保密。还有，可能的密钥序列的数目足够大，以致利用穷举搜索找出正确序列是不实际的。这就是计算保密。

虽然已描述和说明了申请人的发明的具体实施例，但应认识到本发明不受这些实施例的限制。本申请拟包括在所附权利要求书中所规定的申请人的发明的精神实质和范围内的任何以及所有改进。

说 明 书 附 图

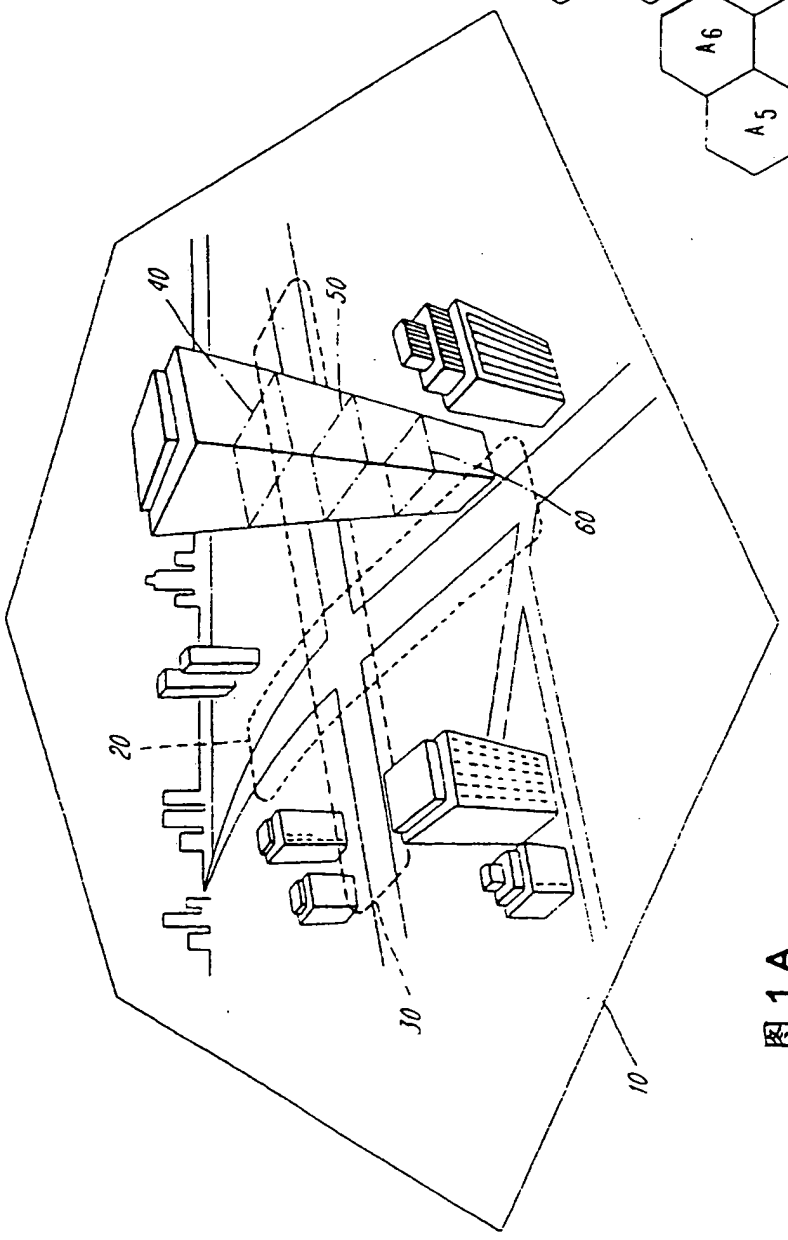


图 1 A

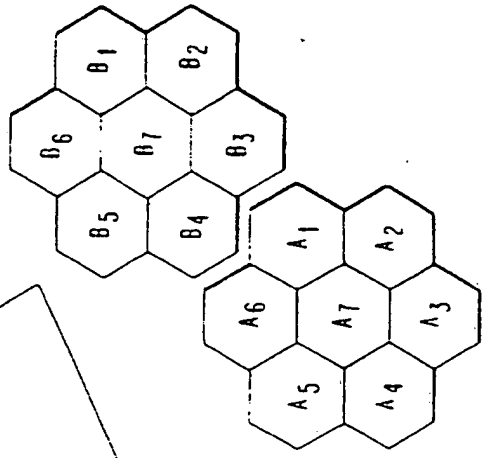


图 1 B
(先有技术)

图 2 A

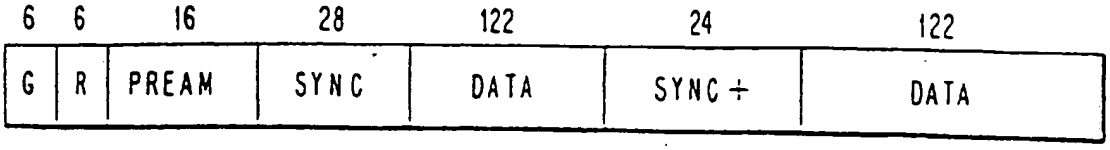


图 2 B

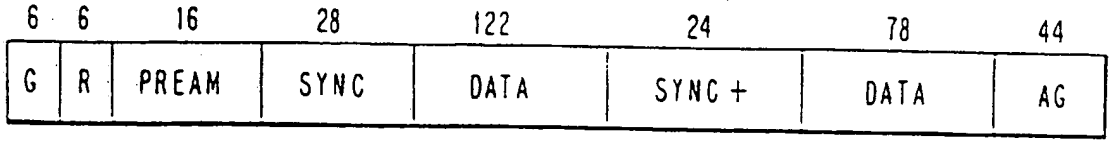
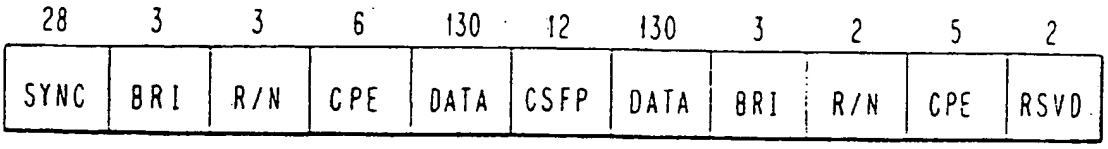
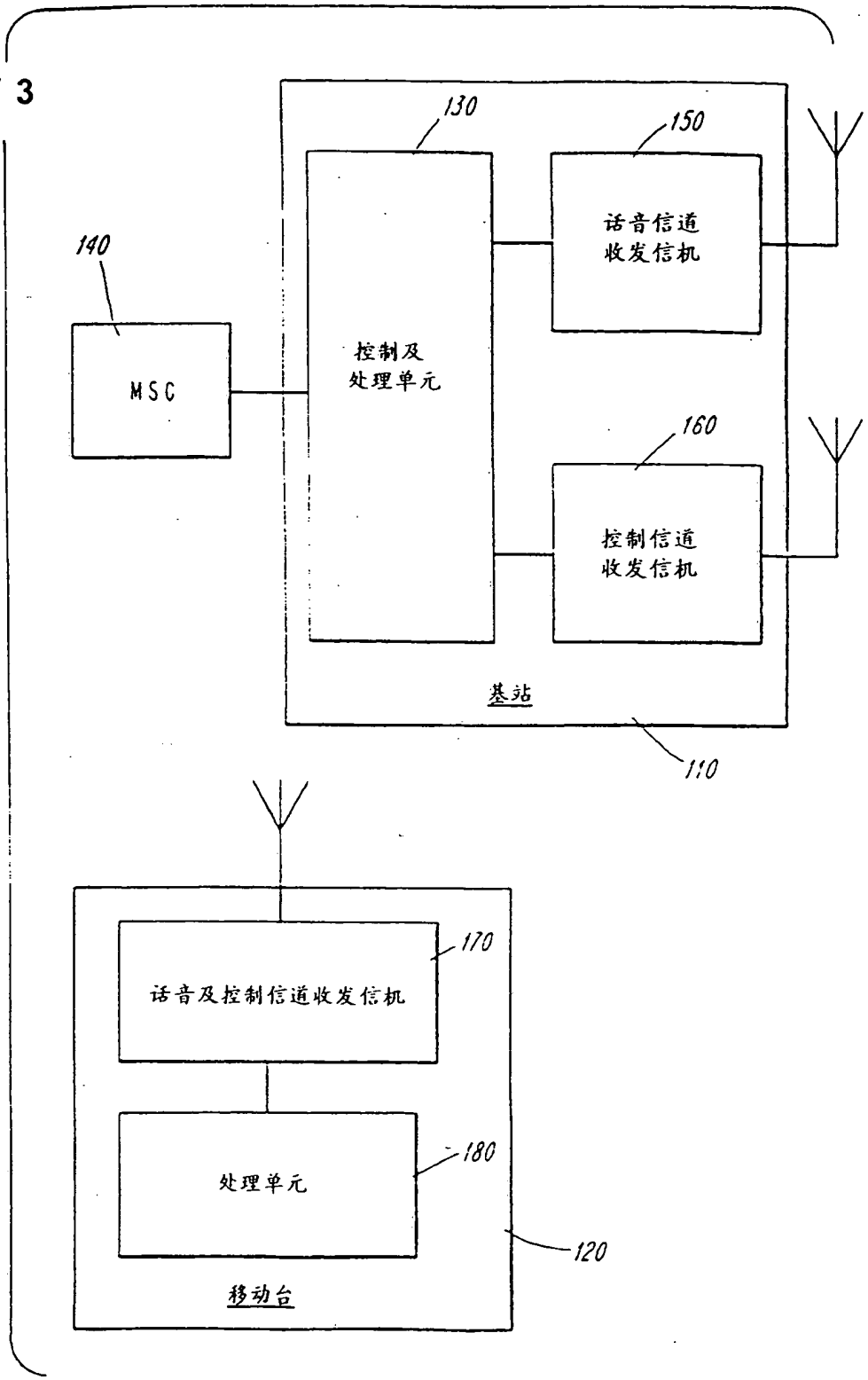


图 2 C



AG = 短缩的保护时间
BRI = 忙/预留/空闲指示符
CSFP = 编码超帧相位
DATA = 信息比特
G = 保护时间
CPE = 编码的部分回波
PREAM = 前导码
R = 斜坡时间
R/N = 接收/不接收
RSVD = 预留字段,置为11
SYNC = 同步
SYNC+ = 附加同步

图 3


130
150
话音信道
收发信机
140
MSC
控制及
处理单元
160
控制信道
收发信机
基站
110
170
话音及控制信道收发信机
180
处理单元
120
移动台

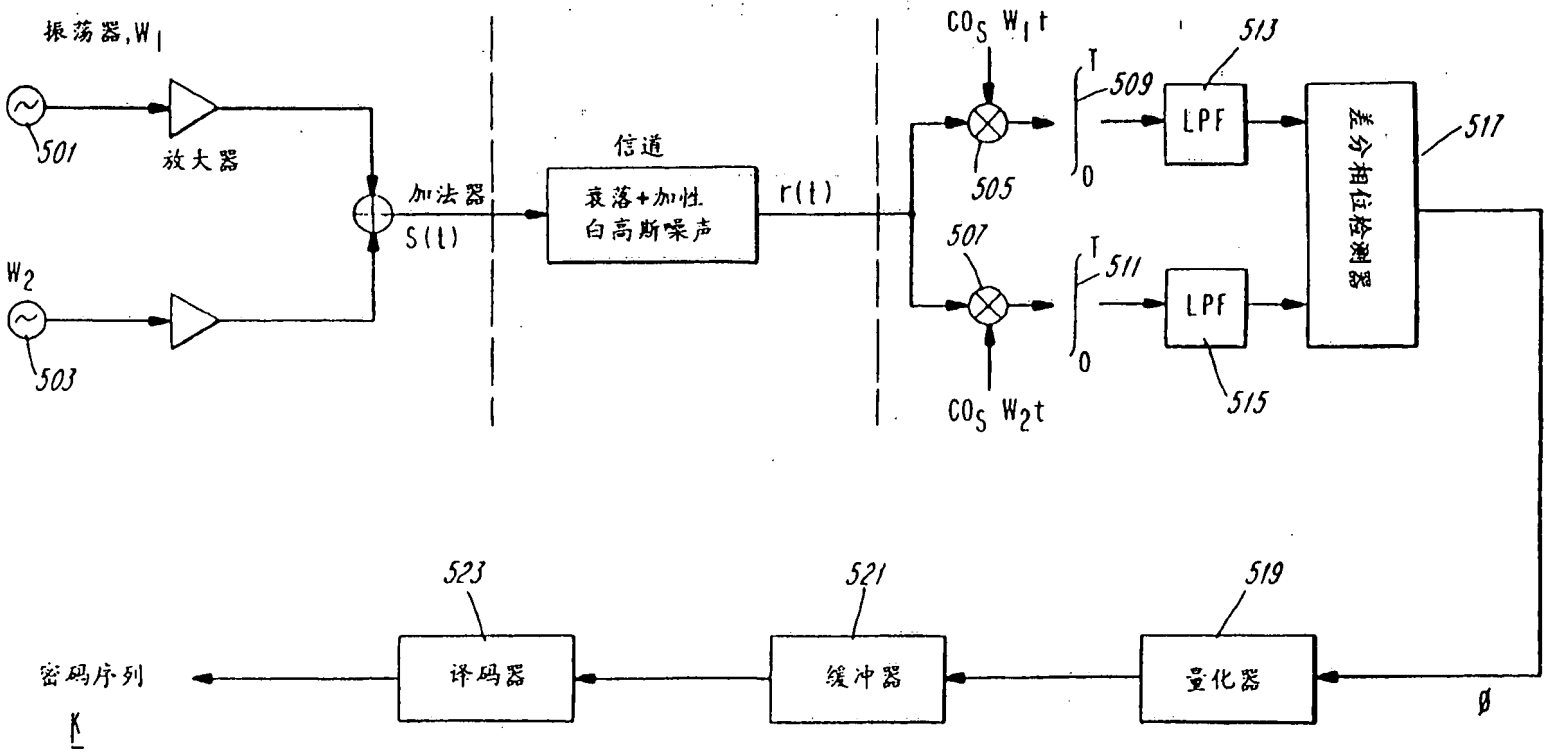

振荡器,W_1
501
放大器
W_2
503
加法器
S(t)
信道
衰落+加性
白高斯噪声
r(t)
$\cos W_1 t$
505
507
$\cos W_2 t$
T
0
509
511
LPF
LPF
513
515
差分相位检测器
517
519
量化器
521
缓冲器
523
译码器
密码序列
K
ϕ

图 5

图 4

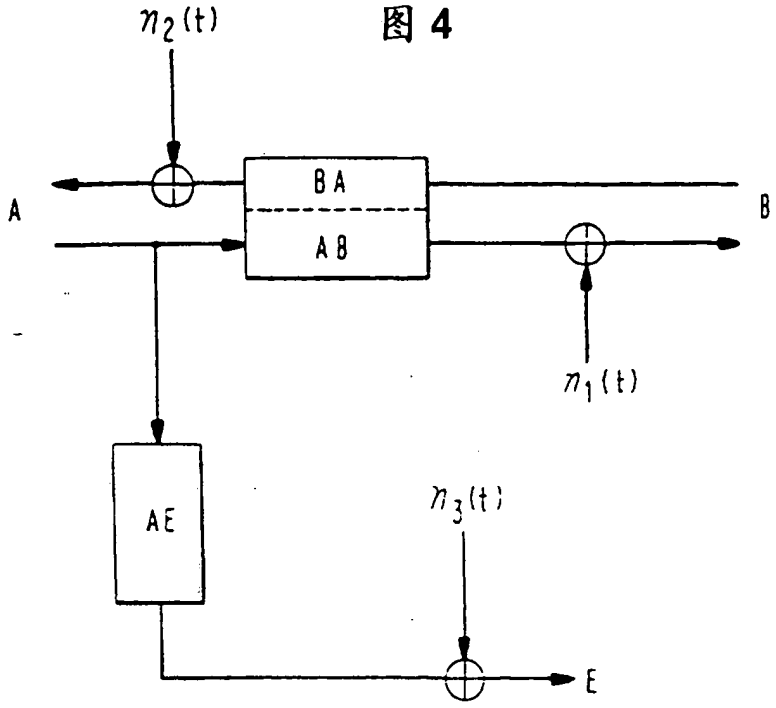


图 6

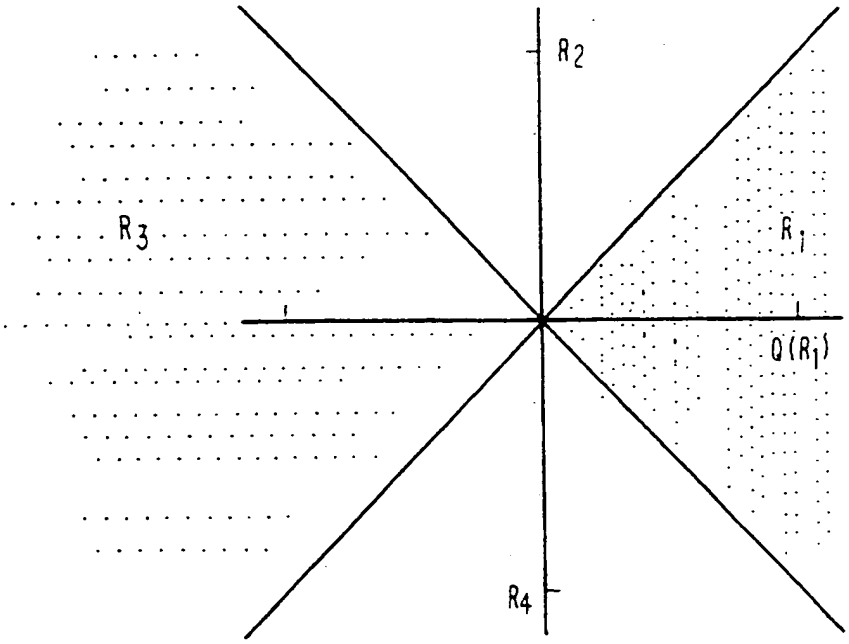


图 7

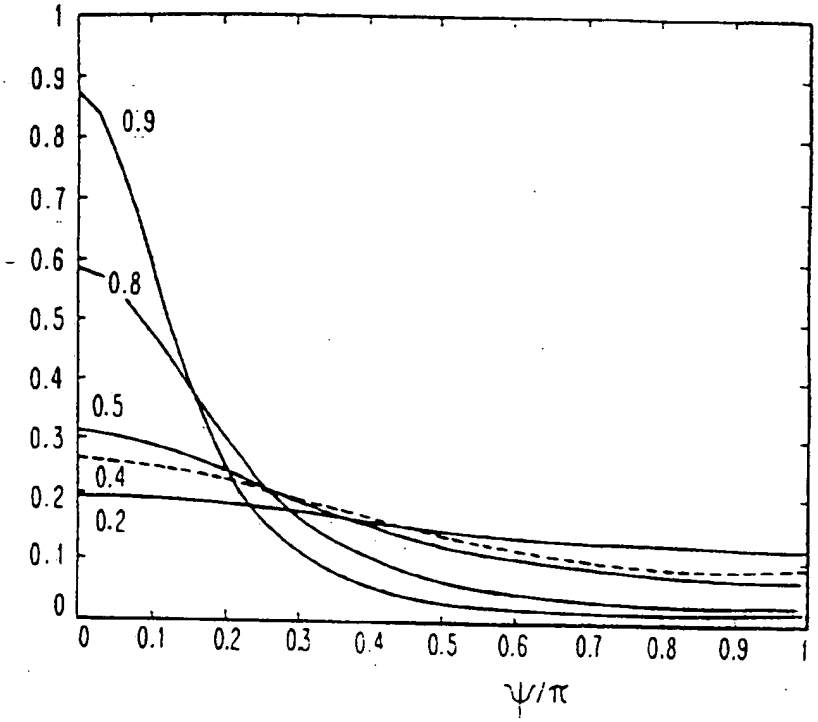
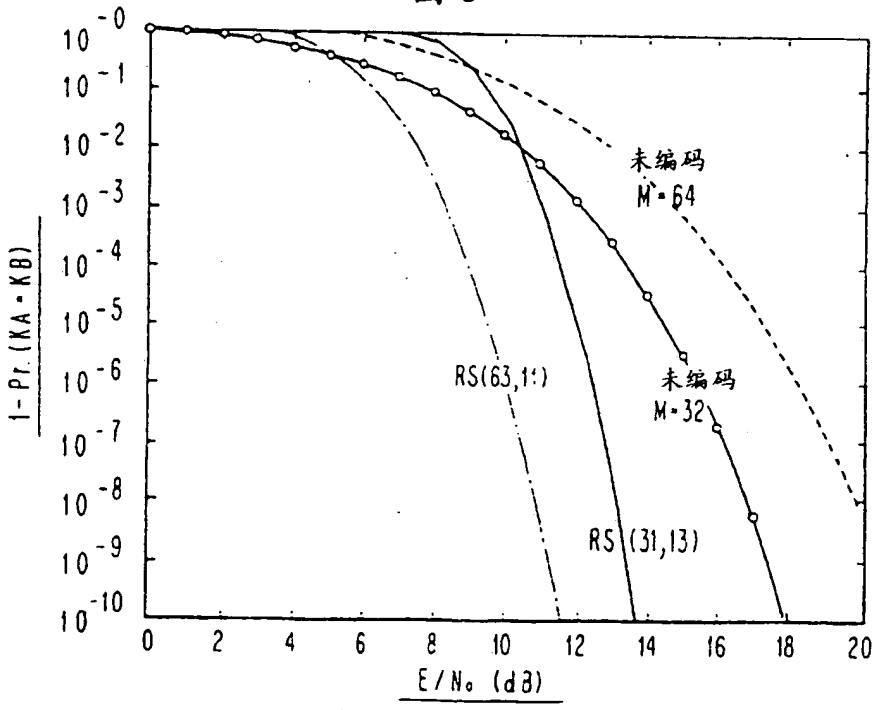


图 9



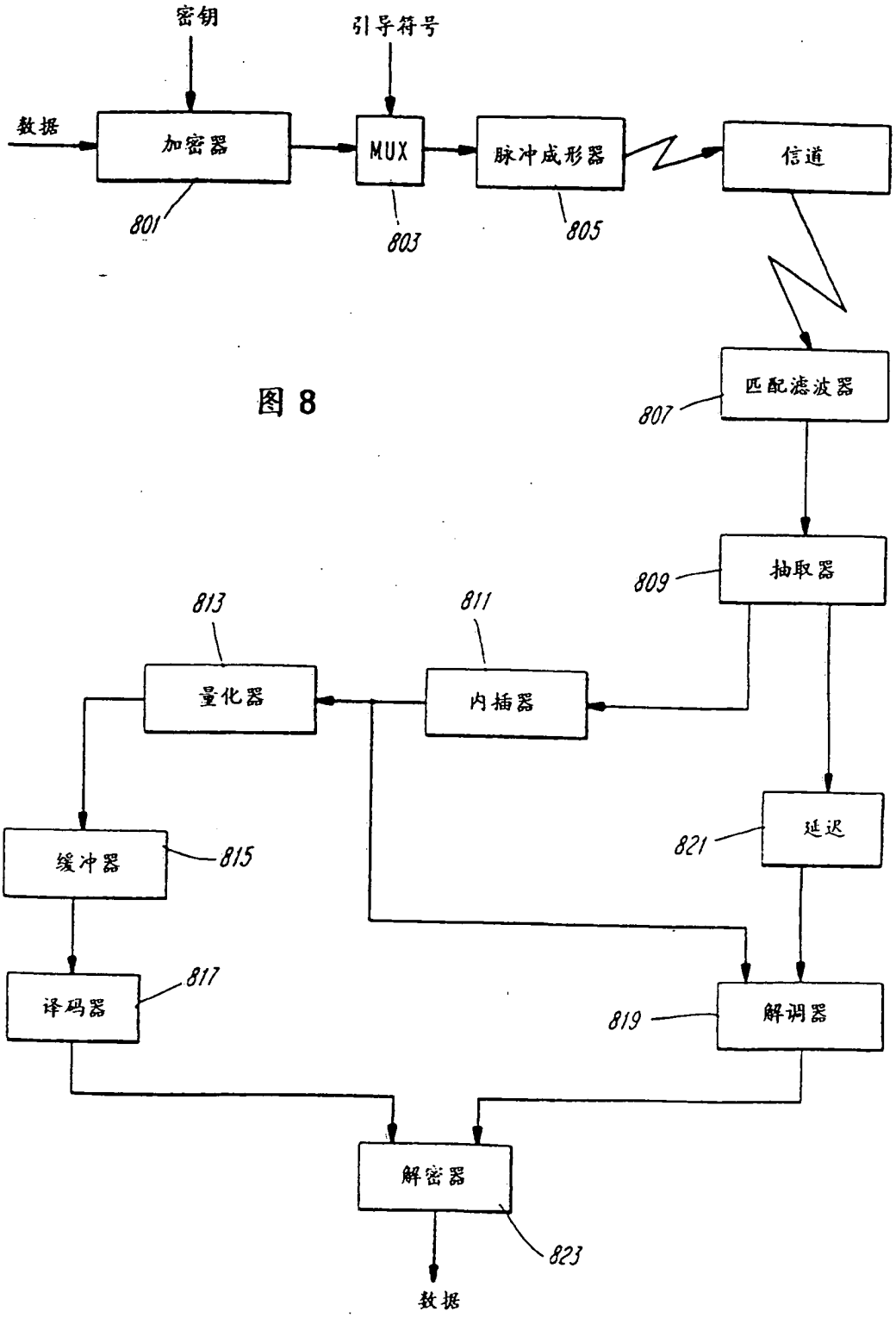

密钥
引导符号
数据
加密器
MUX
脉冲成形器
信道
801
803
805
匹配滤波器
807
抽取器
809
813
811
量化器
内插器
缓冲器
815
延迟
821
译码器
817
解调器
819
解密器
823
数据

图 8